Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1-14. **(Cancelled)**

15. **(Currently Amended)** The method of claim 34, wherein at least one of said ~~corresponding part of~~ operations in the first chain of operations ~~corresponding to the at least a part of the second chain of operation~~ comprises an exclusive OR.

16. **(Currently Amended)** The method of claim [[14]] 34, wherein at least one of said ~~corresponding part of~~ operations in the first chain of operations ~~corresponding to the at least a part of the second chain of operations~~ comprises an operation of bit permutation of an intermediate result obtained ~~by carrying out~~ from execution of operations of said ~~second~~ first chain of operations preceding ~~this~~ said operation of bit permutation.

17. **(Currently Amended)** The method of claim 34, wherein at least one of said ~~corresponding part of~~ operations in the first chain of operations ~~corresponding to the at least a part of the second chain of operations~~ comprises an operation of indexed access to a table.

18. **(Currently amended)** The method of claim 34, wherein at least one of said ~~corresponding part of~~ operations in the first chain of operations ~~corresponding to the at least a part of the second chain of operations~~ comprises an operation which is stable with respect to the application of an exclusive OR function.

19. **(Currently amended)** The method of claim [[18]]34, wherein at least one of said ~~corresponding part of~~ operations in the first chain of operations ~~corresponding to the at least a part of the second chain of operations is~~ comprises an operation of transfer of an intermediate result obtained ~~by carrying out~~from execution of operations of said second chain of operations preceding ~~this~~ said operation of transfer, from one location to another one in a storage space.

20-21. **(Cancelled)**

22. **(Currently amended)** The method of claim [[20]]34, wherein the step of randomly choosing comprises generating ~~selecting is conducted depending on the state of~~ a random parameter that is used to identify which of said groups to choose, ~~generated for each part of the series of several parts within this first chain of operations~~ and wherein said method further comprises updating a complementation counter at each generation of the random parameter, and the step of ~~selecting to output~~ outputting as the resultant message ~~the result of the last operation in either in a same state or in a complemented state~~ is decided depending on ~~the~~ a state of the complementation counter to determine whether to output the result of the last operation in the uncomplemented state or the complemented state as the resultant message.

23. **(Currently amended)** The method of claim [[20]]34, wherein the step of randomly choosing comprises generating ~~selecting is conducted depending on the state of~~ a random parameter that is used to identify which of said groups to choose,~~generated for each part of the series of several parts within this first chain of operations~~ and wherein said method further comprises transmitting, with each executed operation, ~~for each part of said series of~~

~~several parts within this first chain of operations,~~ information to be used during the step of outputting ~~as~~ the resultant message to determine whether to output the result of the last operation in the uncomplemented state or the complemented state as the resultant message ~~the result of the last operation in a same state of in a complemented state~~.

24. **(Currently amended)** The method of claim [[20]]34, wherein the step of randomly ~~selecting~~ choosing comprises a step of computing a parameter which is equal to a difference between ~~the~~ a number of times when an operation of the ~~second~~ first chain of operations is ~~in the same state as in the first chain of operations~~ executed and ~~the~~ a number of times when an operation of the second chain of operations ~~of the chain~~ is ~~in complemented state~~executed, and when ~~this~~ the difference exceeds a given threshold, the step of randomly ~~selecting~~ choosing ~~a next part of the series of several parts in a normal state or in a complemented state~~ is conducted so as to decrease ~~this~~ the difference.

25. - 26. **(Cancelled)**

27. **(Currently amended)** The method of claim 34, wherein the step of storing, at the microcircuit card, a second chain of operations comprises complementing ~~complemented state of said corresponding part of~~ each operation in the first chain of operations ~~corresponding to the at least a part of the second chain of operations is obtained~~ by a complementation carried out byte by byte.

28. **(Currently amended)** The method of claim 34, wherein the step of storing, at the microcircuit card, a second chain of operations comprises complementing ~~complemented state of said corresponding part of~~ each operation in the first chain of

operations ~~corresponding to the at least a part of the second chain of operations is obtained~~ by a complementation carried out bit by bit.

29. **(Currently Amended)**The method of claim 34, wherein the step of having the microcircuit ~~entity~~card determine the second chain of operations further comprises a step of determining a permutation of the order of successive commutative operations in the first chain of operations.

30. **(Previously Presented)** The method of claim 29, wherein the step of determining a permutation of the order of successive commutative operations is carried out randomly.

31. **(Currently amended)** The method of claim [[21]]34, wherein the step of randomly selecting at least one of the operations in the first chain of operations and at least one of the operations in the second chain of operations comprises generating ~~is conducted depending on the state of~~ a random parameter before ~~generated for~~ each operation is selected ~~of the series of several operations within the first chain of operations~~ and ~~comprises~~ updating a complementation counter, and the step of ~~selecting to output~~outputting as the resultant message ~~the result of the last operation in either in a same state or in a complemented state~~ is decided depending of ~~the~~ a state of the complementation counter to determine whether to output the result of the last operation in the uncomplemented state or the complemented state as the resultant message.

32. **(Currently amended)** The method of claim ~~21~~34, wherein the step of randomly selecting at least one of the operations in the first chain of operations and at least one of the operations in the second chain of operations comprises generating ~~is conducted~~

~~depending of the state of~~ a random parameter ~~generated for~~ before each operation ~~of the series of several operations of the first chain of operations~~ is selected and wherein said method further comprises transmitting, with ~~for~~ each executed operation ~~of the series of operations within the first chain of operations~~, information to be used during the step of outputting ~~as~~ the resultant message to determine whether to output the result of the last operation in the uncomplemented state or the complemented state as the resultant message ~~the result of the last operation in a same state or in a complemented state~~.

33. **(Currently amended)** The method of claim [[21]]34, wherein the step of randomly selecting at least one of the operations in said first chain of operations and at least one of the operations in said second chain of operations comprises a step of computing a parameter which is equal to a difference between ~~the~~ a number of times when an operation of the ~~second~~ first chain of operations is ~~in the same state as in the first chain of operations~~ executed and ~~the~~ a number of times when an operation of the second chain of operations is ~~in a complemented state with respect to the first chain of operations~~executed, and when the difference exceeds a given threshold, the step of randomly selecting a next operation of the of the first chain of operations or the second chain of operations ~~in a normal state or in a complemented state~~ is conducted so as to decrease this difference.

34 **(Currently amended)** A method of ~~performing an authentication~~executing and validating a cryptographic protocol between a server entity and a microcircuit ~~entity~~card in order to resist a DPA attack against the microcircuit ~~entity~~card during ~~performing this~~ execution of said ~~authentication~~ cryptographic protocol, said method comprising the steps of:

storing ~~a DES comprising~~ a first chain of operations in both the server entity and the microcircuit ~~entity~~card, said first chain of operations forming a data encryption standard,

storing, at the microcircuit card, a second chain of operations based on the first chain of operations stored in said microcircuit card, said second chain of operations comprising a succession of operations each corresponding to a complement of one of said operations in the first chain of operations,

~~having~~ sending a message ~~exchanged between this~~ from said server entity ~~and this~~ to said microcircuit ~~entity~~card,

~~having~~ executing, at the server entity, ~~apply to the message~~ the first chain of operations ~~which is~~ stored therein using said message ~~so as~~ to obtain a server result, ~~having the microcircuit entity, determine a second chain of operations from the first chain of operations which is stored in this microcircuit entity, this second chain of operations comprising a succession of operations each corresponding to a corresponding operation in the first chain of operations, with each operation of the second chain of operations being the corresponding operation of the first chain of operations either in the same state or in the complemented state the step of having the microcircuit entity, determine the second chain of operations from the first chain of operations comprising a step of randomly selecting, for at least a part of the second chain of operations corresponding to a corresponding part of the first chain of operations, either this at least a part of the operations of the first chain of operations in a same state as in the first chain of operations, or this at least a part of the first chain of operations in a complemented state, the step of having the microcircuit entity, determine the second chain of operations being such that at least some of the operations of this second chain of operations are in the same state as the corresponding operations in the~~

~~first chain of operations whereas the other operations of this second chain of operations are in complemented state with respect to the corresponding operations of the first chain of operations,having~~

identifying, in the microcircuit card, ~~apply this~~ a selected chain of operations, said step of identifying comprising randomly choosing one of the following groups as said selected chain: 1) all of the operations in said first chain of operations; 2) all of the operations in said first chain of operations; or 3) a plurality of operations comprising a random selection of at least one of the operations in said first chain of operations and at least one of the operations in said second chain of operations ~~to the message so as to obtain a resultant message~~,

executing, in the microcircuit card, the identified chain of operations on said message,

~~the step of having the microcircuit, apply this second chain of operations comprisinga step of selecting to output as the resultant message, depending on the step of having the microcircuit entity determine the second chain of operations, one of either the result of~~ outputting a result of a last operation executed in said identified chain of operations either in an uncomplemented state or a complemented state as a resultant message~~of the second chain of operations in a same state or the result of this last operation of the second chain of operation in a complemented state~~, ~~and~~

comparing the resultant message ~~obtained from the second chain of operations~~ to the server result, and

validating the ~~authentication~~ cryptographic protocol between the server entity and the microcircuit ~~entity~~card when the server result and the resultant message are identical.

35. **(Cancelled)**